PROVING THE LAW OF QUADRATIC RECIPROCITY

VÉRONIQUE BOISVERT AND ELIZABETH MALTAIS

Abstract. In this paper, we will be following the historical development of the law of quadratic reciprocity leading up to its proof.

1. Introduction

The law of quadratic reciprocity was an important breakthrough in number theory. It can be stated today in the following form:

For two distinct odd primes, p and q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}, \text{ where } \left(\frac{p}{q}\right) \text{ represents the Legendre symbol of } p \text{ and } q.$$

We will start in Section 2 by giving a brief historical sketch of the problem. In Section 3 notations used in quadratic reciprocity such as the Legendre symbol and its related counterparts will be defined. In Section 4, we will cover some of Euler's conjectures as well as Euler's criterion and the supplements to quadratic reciprocity. We will also discuss Legendre's work on the theorem and outline his attempted proof in Section 5. Section 6 and 7 will give proofs of the main result. To conclude, Section 8 will deal with some applications and examples.

2. History

Euler first stated the theorem in 1783 but without a proof. Legendre gave the first proof in 1785 but it contained errors. And, finally in 1796, Gauss published the first correct proof. [Weisstein, http://mathworld.wolfram.com/Quadratic ReciprocityTheorem.html] Gauss claimed the proof as his own without mentioning that he was improving Legendre's work. Legendre was very hurt by this and wrote:

> This excessive impudence is unbelievable in a man who has sufficient personal merit to have need of appropriating the discoveries of others. [O'Connor]

Gauss published eight proofs of the quadratic reciprocity law throughout his life and claimed this theorem as being his favorite in number theory. According to John Stillwell, this is the most proved theorem in mathematics, after Pythagoras' theorem [Stillwell, p.162]. Today, there are more than 200 proofs published by a large number of mathematicians. The date of publication and authors of the first 196 proofs are listed in the appendix.

3. Notations: Legendre and Jacobi symbols

Definition 3.1. The Legendre symbol, sometimes called the quadratic character symbol, is defined for distinct odd primes p and q by:

$$\left(\frac{p}{q}\right) = \begin{cases} 1 & \text{if p is a quadratic residue of q} \\ -1 & \text{if p is a quadratic non-residue of q} \end{cases}$$

It satisfies the following properties [Weisstein, http://mathworld.wolfram.com/LegendreSymbol.html]:

$$\left(\frac{n}{m}\right)\left(\frac{n'}{m}\right) = \left(\frac{nn'}{m}\right)$$

$$\left(\frac{n^2}{m}\right) = 1$$

$$\left(\frac{n}{m}\right) = \left(\frac{n'}{m}\right) \text{ if } n \equiv n' \mod m$$

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} = \begin{cases} 1 & \text{if } m \equiv 1 \mod 4 \\ -1 & \text{if } m \equiv -1 \mod 4 \end{cases}$$

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} = \begin{cases} 1 & \text{if } m \equiv \pm 1 \mod 8 \\ -1 & \text{if } m \equiv \pm 3 \mod 8 \end{cases}$$

This symbol simplifies the notations while calculating quadratic residues and therefore, has been very useful for the proofs of the law of quadratic reciprocity.

As we study quadratic reciprocity, it is important to be informed about the Jacobi symbol which is a generalization of the Legendre symbol. It first appeared in Jacobi's paper *Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie*, in 1837 [Lemmermeyer].

Definition 3.2. The Jacobi symbol is defined for positive, odd and relatively prime integers n and m (not necessarily primes numbers) as

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)^{a_1}\left(\frac{n}{p_2}\right)^{a_2}\cdots\left(\frac{n}{p_k}\right)^{a_k}$$

where $m = {p_1}^{a_1}{p_2}^{a_2}\ldots{p_k}^{a_k}$ is the prime factorization of m and $\left(\frac{n}{p_i}\right)$ is the Legendre symbol.

The Jacobi symbol satisfies the same properties as the Legendre symbol [Weisstein, http://mathworld.wolfram.com/JacobiSymbol.html].

The quadratic reciprocity law stated at the beginning of this paper is in fact the quadratic reciprocity law of the Legendre symbol.

Theorem 3.3. *The quadratic reciprocity law of the Jacobi symbol is stated as the following* [Komatsu]*:*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}+\frac{sgnm-1}{2}\frac{sgnn-1}{2}}$$

Proposition 3.4. *The properties of the Jacobi symbol are sometimes stated in the following way* [Komatsu]*:*

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}+\frac{sgnn-1}{2}}$$

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n'-1}{4}} \text{ where } n' = (-1)^{\frac{n-1}{2}} n$$

and can be reduced to two of the properties stated above for the Legendre symbol.

Proof.

- 3.4 First Property

  If $n > 0$, then $\frac{sgnn-1}{2} = \frac{1-1}{2} = 0$
  $\Rightarrow \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}+\frac{sgnn-1}{2}} = (-1)^{\frac{n-1}{2}}$

  If $n < 0$, then $\left(\frac{-1}{n}\right) = \left(\frac{-1}{-n}\right)$ since $-1 \equiv a^2 \mod n$ means $-1 - a^2 = kn$ for some k, or equivalently, $(-k)(-n)$ so $-1 \equiv a^2 \mod -n$
  $\Rightarrow \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}+\frac{sgnn-1}{2}} = (-1)^{\frac{n-1}{2}}$

  Therefore, $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$ for all n.

- 3.4 Second Property

  Let's suppose $n \equiv 1 \mod 8$
  $\Rightarrow n = 8k+1 \Rightarrow n' = (-1)^{\frac{8k}{2}}(8k+1)$
  $\Rightarrow \left(\frac{2}{n}\right) = (-1)^{\frac{n'-1}{4}} = (-1)^{\frac{8k}{4}} = 1 = (-1)^{\frac{n^2-1}{8}}$

  Let's suppose $n \equiv -1 \mod 8$
  $\Rightarrow n = 8k-1 \Rightarrow n' = (-1)^{\frac{8k-2}{2}}(8k-1)$
  $\Rightarrow \left(\frac{2}{n}\right) = (-1)^{\frac{n'-1}{4}} = (-1)^{\frac{-8k}{4}} = 1 = (-1)^{\frac{n^2-1}{8}}$

  Let's suppose $n \equiv 3 \mod 8$
  $\Rightarrow n = 8k+3 \Rightarrow n' = (-1)^{\frac{8k+2}{2}}(8k+3)$
  $\Rightarrow \left(\frac{2}{n}\right) = (-1)^{\frac{n'-1}{4}} = (-1)^{\frac{-8k-4}{4}} = -1 = (-1)^{\frac{n^2-1}{8}}$

  Let's suppose $n \equiv -3 \mod 8$
  $\Rightarrow n = 8k-3 \Rightarrow n' = (-1)^{\frac{8k-4}{2}}(8k-3)$
  $\Rightarrow \left(\frac{2}{n}\right) = (-1)^{\frac{n'-1}{4}} = (-1)^{\frac{8k-4}{4}} = -1 = (-1)^{\frac{n^2-1}{8}}$

  Therefore, $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$ for all m and n, relatively prime integers.

□

The Kronecker's symbol is another generalization of the Legendre symbol but it will not be discussed here. From now on, the quadratic reciprocity law discussed will be that of the Legendre symbol.

4. Euler's Criterion

Although Euler offered no proof to the law of quadratic reciprocity, he did make the following conjectures which are equivalent to the theorem [Stillwell]

Let p and q be two distinct odd primes.

- When p and q are both of the form $4n+3$ then p is a square (mod q) $\iff$ q is not a square (mod p).
- Otherwise, p is a square (mod q) $\iff$ q is a square (mod p).

Euler also stated and proved the theorem that is known today as *Euler's criterion*. We will state it here.

Theorem 4.1. *(Euler's Criterion) For an odd prime p, and a an integer relatively prime to p,*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (mod\ p),$$

or, alternatively,

$$a \text{ is a square } (mod\ p) \iff a^{\frac{p-1}{2}} \equiv 1 (mod\ p).$$

Euler gave his proof of this criterion using a result called Fermat's little theorem which then led to the proofs of two special cases of quadratic reciprocity. These are referred to as *the first and second supplements to quadratic reciprocity*, and they examine the quadratic character of -1 and 2 with respect to a given odd prime p. We will now state the supplements.

Theorem 4.2. *(First supplement to quadratic reciprocity)*
For an odd prime p,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p = 4n+1; \\ -1 & \text{if } p = 4n+3. \end{cases}$$

This simply means that -1 is a quadratic residue of primes of the form $4n+1$, and -1 is a quadratic non-residue of primes of the form $4n+3$.

(Second supplement to quadratic reciprocity)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p = 8n \pm 1; \\ -1 & \text{if } p = 8n \pm 3. \end{cases}$$

In this case, 2 is a quadratic residue of primes of the form $8n \pm 1$, and is a quadratic non-residue of primes of the form $8n \pm 3$.

The supplements to quadratic reciprocity can be proven using Euler's criterion. Yet, it should be noted that Fermat seems to have known the quadratic character of 2 with respect to any odd prime even before Euler's Criterion was stated [Stillwell]. It is unclear, however, what methods Fermat based this knowledge on.

5. Adrien-Marie Legendre (1752-1833)

The paper presented to the Academy by Legendre in 1785 contained the following theorems [Lemmermeyer, p.6]:

Theorem 5.1. *Consider the primes $a, A \equiv 1 \mod 4$ and $b, B \equiv 3 \mod 4$*

- *Théorème I Si $b^{\frac{a-1}{2}} = +1$, il s'ensuit $a^{\frac{b-1}{2}} = +1$.*
- *Théorème II Si $a^{\frac{b-1}{2}} = -1$, il s'ensuit $b^{\frac{a-1}{2}} = -1$.*
- *Théorème III Si $a^{\frac{A-1}{2}} = +1$, il s'ensuit $A^{\frac{a-1}{2}} = +1$.*
- *Théorème IV Si $a^{\frac{A-1}{2}} = -1$, il s'ensuit $A^{\frac{a-1}{2}} = -1$.*
- *Théorème V Si $a^{\frac{b-1}{2}} = +1$, il s'ensuit $b^{\frac{a-1}{2}} = +1$.*
- *Théorème VI Si $b^{\frac{a-1}{2}} = -1$, il s'ensuit $a^{\frac{b-1}{2}} = -1$.*

- *Théorème VII Si* $b^{\frac{B-1}{2}} = +1$, *il s'ensuit* $B^{\frac{b-1}{2}} = -1$.
- *Théorème VIII Si* $b^{\frac{B-1}{2}} = -1$, *il s'ensuit* $B^{\frac{b-1}{2}} = +1$.

Legendre gave complete proofs for theorem I, II and VII. The proof of theorem VIII was based on a theorem that was only later proved by Dirichlet: Let a and b be positive integers; if gcd(a,b) = 1, then there exist infinitely many primes $\equiv a$ mod b. Legendre later gave complete proofs of theorem VII and VIII using Pell's equation but never succeeded in giving satisfactory proofs of theorems III-VI. This came from the fact that the role of Dirichlet's theorem in quadratic reciprocity was unclear but Gauss later proved that quadratic reciprocity is in fact a corollary of this theorem [Lemmermeyer, pp.6-8].

6. Gauss' third proof

Gauss finally succeeded in discovering the first complete proof of the law of quadratic reciprocity in 1796. This first proof used induction and was "a long and ugly proof" [Stillwell]. We will not state this proof, but rather, we will give the third published proof of the law (which is actually Gauss' fifth discovered proof, although it was published before his third and fourth) since the latter is considered by Gauss and many others to be "the most direct and elegant of his eight demonstrations" [Smith]. Gauss' pride towards this particular proof can be viewed in the introduction to his third proof wherein he wrote the following:

> For a whole year this theorem tormented me and absorbed my greatest efforts until at last I obtained a proof given in the fourth section of the [*Disquisitiones Arithmeticae*]. Later I ran across three other proofs which were built on entirely different principles. One of these I have already given in the fifth section, the others, which do not compare with it in elegance, I have reserved for future publication. Although these proofs leave nothing to be desired as regards rigor, they are derived from sources much too remote, except perhaps the first, which however proceeds with laborious arguments and is overloaded with extended operations. I do not hesitate to say that till now a *natural* proof has not been produced. I leave it to the authorities to judge whether the following proof which I have recently been fortunate enough to discover deserves this description [Smith].

We will proceed with the proof following Gauss which relies on Gauss' lemma as well as some key results obtained using the floor function to conclude the final result. It is taken from a translation of Gauss' proof contained in David Eugene Smith's publication: A Source Book in Mathematics [Smith].

Theorem 6.1. *(Gauss' lemma) Let p be a positive prime number and let k be any number not divisible by p. That is, gcd(k,p)=1. Further let*

$$A = \left\{1, 2, 3, ..., \frac{(p-1)}{2}\right\} \text{ and let } B = \left\{\frac{(p+1)}{2}, \frac{(p+3)}{2}, ..., p-1\right\}.$$

We determine the smallest positive residue modulo p of the product of k by each of the numbers in the set A. These will be distinct and will belong partly to A and *partly to B. The set of products will be*

$$\left\{k, 2k, 3k, ..., \frac{(p-1)}{2}k\right\} (mod\ p).$$

If we let μ (which is now called the characteristic number [Andrews]*) be the number of these residues belonging to B, then k is a quadratic residue of p or a quadratic non-residue of p according as μ is odd or even.*

ie.

$$\left(\frac{k}{p}\right) = (-1)^{\mu}.$$

Proof. Let $a, a', a'', ...$ be the residues belonging to the set A and $b, b', b'', ...$ be those belonging to B. Then the complements of these latter: $(p-b), (p-b'), (p-b''), ...$ are not equal to any of the numbers $a, a', a'', ...$, for if we take $a = nk \in$ A and $b = mk \in$ B where mk and nk are elements from the set of products $\{tk|t \in A\}$ then $a \equiv p - b(mod\ p) \Longrightarrow nk \equiv p - mk(mod\ p) \Longrightarrow nk \equiv -mk(mod\ p) \Longrightarrow n \equiv -m(mod\ p)$. However, this is impossible since m and n belong to A and hence are both less than $\frac{p-1}{2}$. Thus, the complements $(p-b), (p-b'), (p-b''), ...$ belong to A and are distinct from the numbers $a, a', a'', ...$ and together these numbers make up the $\frac{p-1}{2}$ elements of the set A.

Consequently, we have

$$(1)(2)(3)\cdots\left(\frac{p-1}{2}\right) = (a)(a')(a'')\cdots(p-b)(p-b')(p-b'')\cdots(mod\ p).$$

Since $p-b \equiv -b$ $(mod\ p)$ and since there are μ b^i's, the right-hand product becomes:

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{\mu}(a)(a')(a'')\cdots(b)(b')(b'')\cdots(mod\ p)$$

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{\mu}(k)(2k)(3k)\cdots\frac{(p-1)}{2}k\ (mod\ p)$$

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{\mu}k^{\left(\frac{p-1}{2}\right)}\left(\frac{p-1}{2}\right)!\ (mod\ p)$$

Hence

$$1 \equiv (-1)^{\mu}k^{\left(\frac{p-1}{2}\right)}\ (mod\ p).$$

That is

$$k^{\left(\frac{p-1}{2}\right)} \equiv \pm 1\ (mod\ p)$$

according as μ is even or odd. So our theorem follows from Euler's Criterion (refer to Theorem 4.1).

□

We will now introduce some convenient notations which will be used for the rest of the proof.

- Let the symbol (k, p) represent the number of products among $k, 2k, 3k, ..., \frac{(p-1)}{2}k$ whose smallest positive residue modulo p exceeds $\frac{p}{2}$, that is $(k, p) = \mu$ from Gauss' lemma (Theorem 6.1).
- Further, if x is a non-integral quantity we will express by the symbol $[x]$ the greatest integer less than x so that $x - [x]$ is always a positive quantity between 0 and 1 ie.$[x]$ is the *floor function.*

We can readily establish the following relations using the floor function. The first four are general properties whereas (5)-(9) relate the floor function to congruence classes, the quadratic character of a number with respect to a given prime, and Gauss's lemma. From these we will derive some important results which will lead us to our proof of quadratic reciprocity.

(1) $[x] + [-x] = -1$.
(2) $[x] + b = [x + b]$, whenever b is an integer.
(3) $[x] + [b - x] = b - 1$.
(4) If $x - [x] < \frac{1}{2}$, then $[2x] - 2[x] = 0$.
If $x - [x] > \frac{1}{2}$, then $[2x] - 2[x] = 1$.

We now relate the above relations to congruence classes.

(5) If the smallest positive residue of b $(mod\ p) < \frac{p}{2}$ then $\left[\frac{2b}{p}\right] - 2\left[\frac{b}{p}\right] = 0$.
If the smallest positive residue of b $(mod\ p) > \frac{p}{2}$ then $\left[\frac{2b}{p}\right] - 2\left[\frac{b}{p}\right] = 1$.
(6) From (5), we use the products $k, 2k, 3k, ..., \frac{p-1}{2}k$ as different values for b and add them up. This gives us the total number of these products whose smallest positive residue is greater than $\frac{p}{2}$. Now recall from Gauss' lemma (Theorem 6.1) that this number is μ, the characteristic number of k with respect to p. That is

$$(k,p) = \left[\frac{2k}{p}\right] + \left[\frac{4k}{p}\right] + \left[\frac{6k}{p}\right] + ... + \left[\frac{(p-1)k}{p}\right] - 2\left[\frac{k}{p}\right] - 2\left[\frac{2k}{p}\right] - 2\left[\frac{3k}{p}\right] ... - 2\left[\frac{(p-1)k/2}{p}\right].$$

(7) The following lemma demonstrates the relationship between $\left(\frac{k}{p}\right)$ and $\left(\frac{-k}{p}\right)$.

Lemma 6.2.
$$\left(\frac{k}{p}\right) = \left(\frac{-k}{p}\right) \iff \frac{p-1}{2} \textit{ is even. ie. } p = 4n+1.$$
$$\left(\frac{k}{p}\right) = -\left(\frac{-k}{p}\right) \iff \frac{p-1}{2} \textit{ is odd. ie. } p = 4n+3.$$

Proof. From (6) and (1) we obtain without difficulty

$$(k,p) + (-k,p) = -\frac{p-1}{2} + 2\frac{p-1}{2}$$

Hence,

$$(k,p) + (-k,p) = \frac{p-1}{2} \quad (*)$$

From $(*)$:

- If $p = 4n+1$, then $\frac{p-1}{2}$ will be even. Thus (k,p) and $(-k,p)$ must both be even or both be odd since they add up to an even number. Recall from Gauss' lemma (Theorem 6.1) that (k,p) even $\Longrightarrow \left(\frac{k}{p}\right) = 1$ and (k,p) odd $\Longrightarrow \left(\frac{k}{p}\right) = -1$.
So when (k,p) and $(-k,p)$ are both even we have
$$\left(\frac{k}{p}\right) = 1 = \left(\frac{-k}{p}\right),$$

and when they are both odd we have

$$\left(\frac{k}{p}\right) = -1 = \left(\frac{-k}{p}\right).$$

- If $p = 4n+3$, then $\frac{p-1}{2}$ will be odd. So the sum $(k,p)+(-k,p)$ is odd and it follows that one of (k,p) and $(-k,p)$ must be odd and the other must be even

□

Corollary 6.3. *It is evident that in the first case, -1 is a quadratic residue and in the second a quadratic non-residue of p since we know that $(1,p)$ is always even. This is another derivation of the first supplement to quadratic reciprocity(refer to Theorem 4.2).*

(8) Our next lemma provides us with another formula for (k,p).

Lemma 6.4. • *When p is of the form $4n+1$,*

$$\begin{aligned}(k,p) = &\frac{(k-1)(p-1)}{4}\\ &-2\left\{\left[\frac{k}{p}\right]+\left[\frac{3k}{p}\right]+\left[\frac{5k}{p}\right]+...+\left[\frac{(p-3)k/2}{p}\right]\right\}\\ &-\left\{\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]+...+\left[\frac{(p-1)k/2}{p}\right]\right\}\end{aligned}$$

- *When p is of the form $4n+3$*

$$\begin{aligned}(k,p) = &\frac{(k-1)(p+1)}{4}\\ &-2\left\{\left[\frac{k}{p}\right]+\left[\frac{3k}{p}\right]+\left[\frac{5k}{p}\right]+...+\left[\frac{(p-1)k/2}{p}\right]\right\}\\ &-\left\{\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]+...+\left[\frac{(p-1)k/2}{p}\right]\right\}\end{aligned}$$

Proof. We transform the formula given in (6) as follows: From (3) we have

$$\left[\frac{(p-1)k}{p}\right] = k-1-\left[\frac{k}{p}\right],$$

$$\left[\frac{(p-3)k}{p}\right] = k-1-\left[\frac{3k}{p}\right],$$

$$\left[\frac{(p-5)k}{p}\right] = k-1-\left[\frac{5k}{p}\right],...$$

where we have set

$$b = k \text{ and } x = \frac{(p-i)k}{p} \text{ for } i = 1,3,5,...$$

When p is of the form $4n+1$, we apply these substitutions to the $\frac{p-1}{4}$ corresponding terms as follows:

From (6) we have

$$(k,p) = \left[\frac{2k}{p}\right]+\left[\frac{4k}{p}\right]+...+\left[\frac{(p-5)k}{p}\right]+\left[\frac{(p-3)k}{p}\right]+\left[\frac{(p-1)k}{p}\right]-2\left[\frac{k}{p}\right]-2\left[\frac{2k}{p}\right]...-2\left[\frac{(p-1)k/2}{p}\right].$$

We make the substitutions to get

$$(k,p)=\left[\frac{2k}{p}\right]+\left[\frac{4k}{p}\right]+...+k-1-\left[\frac{5k}{p}\right]+k-1-\left[\frac{3k}{p}\right]+k-1-\left[\frac{k}{p}\right]-2\left[\frac{k}{p}\right]-2\left[\frac{2k}{p}\right]...-2\left[\frac{(p-1)k/2}{p}\right].$$

When we gather like terms we have

$$(k,p)=\frac{(k-1)(p-1)}{4}-2\left[\frac{k}{p}\right]-\left[\frac{k}{p}\right]-2\left[\frac{2k}{p}\right]+\left[\frac{2k}{p}\right]-2\left[\frac{3k}{p}\right]-\left[\frac{3k}{p}\right]...$$

$$-2\left[\frac{(p-3)k/2}{p}\right]-\left[\frac{(p-3)k/2}{p}\right]-2\left[\frac{(p-1)k/2}{p}\right]+\left[\frac{(p-1)k/2}{p}\right],$$

and consequently,

$$(k,p)=\frac{(k-1)(p-1)}{4}$$

$$-2\left\{\left[\frac{k}{p}\right]+\left[\frac{3k}{p}\right]+\left[\frac{5k}{p}\right]+...+\left[\frac{(p-3)k/2}{p}\right]\right\}$$

$$-\left\{\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]+...+\left[\frac{(p-1)k/2}{p}\right]\right\}.$$

Similarly, when p is of the form $4n+3$, we apply such substitutions; however, we apply them to $\frac{p+1}{4}$ terms instead of $\frac{p-1}{4}$ terms. □

(9)

Corollary 6.5. *In the special case $k=2$ it follows from lemma 6.4 that*

$$(2,p)=\begin{cases}\frac{p-1}{4} & \text{if } p=4n+1\\ \frac{p+1}{4} & \text{if } p=4n+3\end{cases},$$

which is equivalent to the second supplement to quadratic reciprocity (Refer to Theorem 4.2). This works out for 2 since each term in the square brackets of our lemma is less than 1 and thus each floor function goes to zero.

Our next theorem will provide us with a relationship between certain floor functions and the reciprocals of those floor functions, keeping in mind that quadratic *reciprocity* is our main goal!

Theorem 6.6. *If x is a positive non-integral quantity such that none of $x, 2x, 3x, ..., nx$ are integers, and we let $[nx]=b$ then none of the multiples of the reciprocals $\frac{1}{x}, \frac{2}{x}, \frac{3}{x}, ..., \frac{b}{x}$ are integers, and we can say that:*

$$nb=\begin{cases}[x]+[2x]+[3x]+...+[nx]\\ +\left[\frac{1}{x}\right]+\left[\frac{2}{x}\right]+\left[\frac{3}{x}\right]+...+\left[\frac{b}{x}\right]\end{cases}$$

Proof. Let $\Omega=[x]+[2x]+[3x]+...+[nx]$. In this series, all the terms from the first up to and including the $\left[\frac{1}{x}\right]^{th}$ are zero, the following terms up to and including the $\left[\frac{2}{x}\right]^{th}$ are equal to 1, and the following up to the $\left[\frac{3}{x}\right]^{th}$ term are equal to 2 and so on. Hence we have

$$\Omega = \left.\begin{array}{l} 0 \times \left[\frac{1}{x}\right] \\ +1 \times \left\{\left[\frac{2}{x}\right] - \left[\frac{1}{x}\right]\right\} \\ +2 \times \left\{\left[\frac{3}{x}\right] - \left[\frac{2}{x}\right]\right\} \\ +3 \times \left\{\left[\frac{4}{x}\right] - \left[\frac{3}{x}\right]\right\} \\ \cdot \\ \cdot \\ \cdot \\ +(b-1) \times \left\{\left[\frac{b}{x}\right] - \left[\frac{b-1}{x}\right]\right\} \\ +b \times \left\{n - \left[\frac{b}{x}\right]\right\} \end{array}\right\} = -\left[\frac{1}{x}\right] + \left[\frac{2}{x}\right] - 2\left[\frac{2}{x}\right] + 2\left[\frac{3}{x}\right] - 3\left[\frac{3}{x}\right] + ... + (b-1)\left[\frac{b}{x}\right] - b\left[\frac{b}{x}\right] + bn$$

Thus,

$$\Omega = bn - \left[\frac{1}{x}\right] - \left[\frac{2}{x}\right] - \left[\frac{3}{x}\right] - ... - \left[\frac{b}{x}\right].$$

□

This next theorem connects Theorem 6.6 to quadratic reciprocity.

Theorem 6.7. *If k and p are positive odd numbers which are relatively prime to each other, we have*

$$\left.\begin{array}{l} \left[\frac{k}{p}\right] + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] + ... + \left[\frac{(p-1)k/2}{p}\right] \\ + \left[\frac{p}{k}\right] + \left[\frac{2p}{k}\right] + \left[\frac{3p}{k}\right] + ... + \left[\frac{(k-1)p/2}{k}\right] \end{array}\right\} = \frac{(k-1)(p-1)}{4}.$$

Proof. Supposing that $k < p$ we have

$$\frac{k(p-1)/2}{p} < \frac{k}{2} \text{ but } \frac{k(p-1)/2}{p} > \frac{k-1}{2} \Longrightarrow \left[\frac{k(p-1)/2}{p}\right] = \frac{k-1}{2}$$

From this it is clear that the theorem follows at once from theorem 6.6 if we set

$$\frac{k}{p} = x, \frac{p-1}{2} = n, \frac{k-1}{2} = b.$$

□

We note that it is possible to prove in a similar way that if k is even and relatively prime to p then

$$\left.\begin{array}{l} \left[\frac{k}{p}\right] + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] + ... + \left[\frac{(p-1)k/2}{p}\right] \\ + \left[\frac{p}{k}\right] + \left[\frac{2p}{k}\right] + \left[\frac{3p}{k}\right] + ... + \left[\frac{kp/2}{k}\right] \end{array}\right\} = \frac{(k)(p-1)}{4}.$$

However we will not prove this proposition as it is not necessary for our purpose.

Now the main theorem follows from the combination of theorem 6.7 with lemma 6.4 as well as the following lemma.

Lemma 6.8. *If k and p are any distinct, positive prime numbers (not equal to 2), and we set*

$$L = (k,p) + \left[\frac{k}{p}\right] + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] + ... + \left[\frac{(p-1)k/2}{p}\right]$$

$$M = (p,k) + \left[\frac{p}{k}\right] + \left[\frac{2p}{k}\right] + \left[\frac{3p}{k}\right] + ... + \left[\frac{(k-1)p/2}{k}\right]$$

then L and M will always be even numbers.

Proof. From lemma 6.4, there are two cases for L: $p = 4n + 1$ and $p = 4n + 3$.

- When $p = 4n + 1$,
$$L = (k, p) + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] + ... + \left[\frac{(p-1)k/2}{p}\right].$$
Notice that $(k, p) - L$ is exactly the last line in the sum in lemma 6.4 and these terms will cancel. From the fact that k is of the form $2m + 1$ (odd), we have
$$\begin{aligned} L &= \frac{(k-1)(p-1)}{4} - 2\left\{\left[\frac{k}{p}\right] + \left[\frac{3k}{p}\right] + \left[\frac{5k}{p}\right] + ... + \left[\frac{(p-3)k/2}{p}\right]\right\} \\ &= \frac{(2m)(4n)}{4} - 2[\cdots] \\ &= 2[mn - [\cdots]] \text{ which is even.} \end{aligned}$$
- When $p = 4n + 3$, a similar argument shows that $L = 2[m(n + 1) - [\cdots]]$ which is even.
- The same arguments work for M in both cases.

□

Now it follows from theorem 6.7 and lemma 6.8 that
$$L + M = (k, p) + (p, k) + \frac{(k-1)(p-1)}{4}.$$
Therefore, $\frac{(k-1)(p-1)}{4}$ is even when one or both of the primes k or p is of the form $4n + 1$. This means that (p, k) and (k, p) are either both even or both odd.

On the contrary, $\frac{(k-1)(p-1)}{4}$ is odd when k and p are both of the form $4n + 3$. Then, necessarily one of (p, k), and (k, p) is even and the other odd.

In the first case, the relations of k to p, and of p to k (as regards to the quadratic character of one of with respect to the other) are the same. In the second case they are opposite. Thus we have the law of quadratic reciprocity.

Q.E.D.

7. General overview of quadratic reciprocity as a proof

The following is an overview of Euler's work on quadratic reciprocity that uses examples and generalizations in order to be presented in the form of a proof. This helps us to better visualize what the law really implicates. It is taken from the paper entitled Quadratic Reciprocity: Its Conjecture and Application written by David A. Cox [Cox] from the Department of Mathematics at Amherst College and published in 1988.

Euler proved the following theorems where p is an odd prime. The theorems were first stated by Fermat and were really useful for the proof of quadratic reciprocity. [Cox, (0.3)]:

Theorem 7.1.
$p = x^2 + y^2, x, y \in \mathbb{Z} \Leftrightarrow p \equiv 1 \mod 4$
$p = x^2 + 2y^2, x, y \in \mathbb{Z} \Leftrightarrow p \equiv 1, 3 \mod 8$
$p = x^2 + 3y^2, x, y \in \mathbb{Z} \Leftrightarrow p = 3 \; or \; p \equiv 1 \mod 3$

From these theorems, came the next very important lemma [Cox, lemma 1.1].

Lemma 7.2. *Let p be a prime not dividing n. Then there are relatively prime integers x and y such that $p|(x^2+ny^2)$ if and only if $\left(\frac{-n}{p}\right)=1$, where $\left(\frac{-n}{p}\right)$ is the Legendre symbol.*

Proof. Let's suppose that $\left(\frac{-n}{p}\right)=1$.
$\exists a \in \mathbb{Z}$ such that $-n \equiv a^2 \mod p$
$\Rightarrow a^2+n \equiv 0 \mod p$
Let $x=a$ and $y=1$
$\Rightarrow p \mid (x^2+ny^2)$

Now, let's suppose that $p \mid (x^2+ny^2)$
$\Rightarrow x^2+ny^2 \equiv 0 \mod p$
$\Rightarrow x^2 \equiv -ny^2 \mod p$
p does not divide n and $(x,y)=1$, therefore p does not divide y
also, p is prime, therefore $(p,y)=1$ and $\exists b$ such that $yb \equiv 1 \mod p$
$\Rightarrow x^2b^2 \equiv -ny^2b^2 \mod p$
$\Rightarrow (xb)^2 \equiv -n(yb)^2 \mod p$
$\Rightarrow (xb)^2 \equiv -n \mod p$
$\Rightarrow \left(\frac{-n}{p}\right)=1$ □

Lemma 7.2 and Theorem 7.1 imply that [Cox, (1.2)]:

$$\left(\frac{-1}{p}\right)=1 \Leftrightarrow p \equiv 1 \mod 4$$
$$\left(\frac{-2}{p}\right)=1 \Leftrightarrow p \equiv 1,3 \mod 8$$
$$\left(\frac{-3}{p}\right)=1 \Leftrightarrow p \equiv 1 \mod 3$$

We find that in order to notice a pattern, we must work modulo 4n. If we search for all primes p for which $\left(\frac{5}{p}\right)=1$, we notice that they are all congruent to 1 or 11 mod 20. Here are some examples (we treat the case where n $\neq$ 1,2 and p does not divide n) [Cox, (1.3)]:

$$\left(\frac{-3}{p}\right)=1 \Leftrightarrow p \equiv 1,7 \mod 12$$
$$\left(\frac{-5}{p}\right)=1 \Leftrightarrow p \equiv 1,3,7,9 \mod 20$$
$$\left(\frac{-7}{p}\right)=1 \Leftrightarrow p \equiv 1,9,11,15,23,25 \mod 28$$
$$\left(\frac{3}{p}\right)=1 \Leftrightarrow p \equiv \pm 1 \mod 12$$
$$\left(\frac{5}{p}\right)=1 \Leftrightarrow p \equiv \pm 1, \pm 11 \mod 20$$
$$\left(\frac{7}{p}\right)=1 \Leftrightarrow p \equiv \pm 1, \pm 3, \pm 9 \mod 28$$

Since, for example, $11 \equiv -9 \mod 20$, the bottom three examples stated above are equivalent to [Cox, (1.4)]:

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \mod 12$$
$$\left(\frac{5}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pm 9 \mod 20$$
$$\left(\frac{7}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1, \pm 25, \pm 9 \mod 28$$

We notice that p is congruent to odd squares! But we must be careful, this is only the case when n is prime. For example, $\left(\frac{6}{p}\right) = 1 \Leftrightarrow p \equiv 1, 5 \mod 24$. We can now generalize with the following conjecture which we will then prove is equivalent to the law of quadratic reciprocity:

If p and q are distinct odd primes, then

$$\left(\frac{q}{p}\right) = 1 \Leftrightarrow p \equiv \pm\beta^2 \mod 4q \text{ for some odd } \beta \tag{7.1}$$

Let p and q be distinct odd primes and set $p* = (-1)^{\frac{p-1}{2}}p$ (Note that $p* \equiv 1 \mod 4$). We assume the following properties:

$$\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}} \text{ (see thm 4.2)}$$
$$\left(\frac{ab}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{b}{q}\right)$$
$$\Rightarrow \left(\frac{p*}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

Therefore, we need to prove either

$$\left(\frac{q}{p}\right) = \left(\frac{p*}{q}\right) \text{ or } \left(\frac{q}{p}\right) = 1 \Leftrightarrow \left(\frac{p*}{q}\right) = 1$$

in order to prove the law of quadratic reciprocity.

By comparing this with (7.1), we see that, in fact, we need to prove

$$\left(\frac{p*}{q}\right) = 1 \Leftrightarrow p \equiv \pm\beta^2 \mod 4q \text{ for some odd } \beta \tag{7.2}$$

If β is odd, then $\beta^2 \equiv 1 \mod 4$, so the $\pm$ sign must be $(-1)^{\frac{p-1}{2}}$. Hence,

$$p \equiv \pm\beta^2 \mod 4q \Leftrightarrow p \equiv (-1)^{\frac{p-1}{2}}\beta^2 \mod 4q \Leftrightarrow p* \equiv \beta^2 \mod 4q$$

So let's prove (7.2) as the following:

$$\left(\frac{p*}{q}\right) = 1 \Leftrightarrow p* \equiv \beta^2 \mod 4q$$

Suppose $p* \equiv \beta^2 \mod 4q$. This implies $p* \equiv \beta^2 \mod q$, so $\left(\frac{p*}{q}\right) = 1$ follows immediately. Conversely, lets suppose $\left(\frac{p*}{q}\right) = 1$. Then $p* \equiv \alpha^2 \mod q$ for some α. Let $\beta = \alpha$ or $\alpha + q$, depending on whether α is even or odd, we get $p* \equiv \beta^2$

mod $4q$, (by Lemma 7.3 and Lemma 7.4) and we have proven the law of quadratic reciprocity!!

Lemma 7.3. *If α is even, then set $\beta = \alpha$ and conclude that $p* \equiv \beta^2 \mod 4q$.*

Proof. (Use the Chinese Remainder Theorem.) □

Lemma 7.4. *If α is odd, then set $\beta = \alpha + q$ and conclude that $p* \equiv \beta^2 \mod 4q$.*

Proof. (Use the Chinese Remainder Theorem.) □

8. Applications and examples

8.1. **Evaluation of the Legendre symbol.** Quadratic reciprocity is very useful to simplify the evaluation of a Legendre symbol.

Example. $\left(\frac{12}{10005007}\right)$ may seem difficult to evaluate at first but, thanks to the law of quadratic reciprocity, we can find that
$\left(\frac{12}{10005007}\right) = \left(\frac{3}{10005007}\right)\left(\frac{4}{10005007}\right) = \left(\frac{3}{10005007}\right)$
$= (-1)^{\frac{3-1}{2}\frac{10005007-1}{2}}\left(\frac{10005007}{3}\right) = -\left(\frac{10005007}{3}\right)$
Since $10005007 \equiv 1 \mod 3$, $\left(\frac{10005007}{3}\right) = \left(\frac{1}{3}\right) = 1$. Therefore, $\left(\frac{3}{10005007}\right) = -1$.

8.2. **More supplements to quadratic reciprocity.** Quadratic reciprocity also helps us in such problems as trying to find every odd prime p for which a, also an odd prime, is a quadratic residue mod p.

Example. [Pong] Let's determine the set of all odd primes p such that $\left(\frac{3}{p}\right) = 1$.
Since

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}\frac{3-1}{2}} = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv -1 \mod 4 \end{cases}$$

we have,

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{if } p \equiv 1 \mod 4 \\ -\left(\frac{p}{3}\right) & \text{if } p \equiv -1 \mod 4 \end{cases}$$

But $\left(\frac{p}{3}\right) = 1 \Leftrightarrow p \equiv 1 \mod 3$
So, $\left(\frac{3}{p}\right) = 1$ if either of the two following statements are true:

- $p \equiv 1 \mod 3$ and $p \equiv 1 \mod 4 \Rightarrow p \equiv 1 \mod 12$
- $p \equiv -1 \mod 3$ and $p \equiv -1 \mod 4 \Rightarrow p \equiv -1 \mod 12$

Therefore, $\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \mod 12$.

8.3. **The method of excludents.** Suppose we have established that a certain number, say r is a quadratic residue of a prime p using the law of quadratic reciprocity. If we wish to find a square which leaves r as a remainder when divided by p, then we may use *the method of excludents* [Beiler].

We know that $x^2 \equiv r(mod\ p) \iff r + py = x^2$, for some multiple y of p. The method of excludents allows us to look at $r + py$ with respect to some arbitrary small modulus, E, and exclude values of y for which $r + py$ is not a square (mod E). We repeat this with other choices for E until a value for y is deduced.

It should be noted that values of y greater than $p/4$ need never be tried since x is a solution $\implies p-x$ is another solution. Hence x or $p-x < p/2 \implies x^2$ or $(p-$

$x)^2 < p^2/4$. Therefore py must be less than $p^2/4$, so $y < p/4$.

Example. Given that $\left(\frac{17}{263}\right) = 1$, let's find y such that $17 + 263y = x^2$. We use E=3 to start. First, $17 + 263y$ becomes $2 + 2y$ (mod 3). Possible values for y are 0, 1, or 2 (mod 3) and using these values for y, possible values of $2 + 2y$ become 2, 1, or 0 (mod 3). However, only 0, and 1 are quadratic residues of 3. This means that the values of y which make $2 + 2y \equiv 2$ $(mod\ 3)$ must be excluded, and y can only be congruent to 1 or 2 (mod 3). Therefore, we exclude values of y of the form $3k$.

Similarly, we can take E=5. Then $17 + 263y \equiv 2 + 2y$ $(mod\ 5)$, and we find that values of y of the form $5k$, and $5k + 2$ may be excluded.

If we repeat this process once more using E=7, we exclude values of y of the form $7k, 7k + 4$, and $7k + 6$.

For $p = 263$, we need to consider numbers less than $263/4 = 65$ as candidates for the value of y. However, we can exclude all multiples of 3, and our list of candidates becomes: 1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26, 28, 29, 31, 32, 34, 35, 37, 38, 40, 41, 43, 44, 46, 47, 49, 50, 52, 53, 55, 56, 58, 59, 61, 62, 64, 65.

Then we delete any which are of the form $5k$ or $5k + 2$ and are left with: 1, 4, 8, 11, 13, 14, 16, 19, 23, 26, 28, 29, 31, 34, 38, 41, 43, 44, 46, 49, 53, 56, 58, 59, 61, 64.

Next, we delete any numbers of the form $7k, 7k + 4$ and $7k + 6$ to get: 1, 8, 16, 19, 23, 26, 29, 31, 38, 43, 44, 59, 61, 64.

The third value in this list works! If we let $y = 16$, then we have

$$17 + 263y = 17 + 263(16) = 4225 = 65^2.$$

And we also have another solution: $263 - x = 263 - 65 = 198$ and we find that $198^2 = 263(149) + 17$.

APPENDIX [Lemmermeyer, Appendix B]

The following table lists the authors of the first 196 proofs of the quadratic reciprocity law as well as the dates of publication. It also reveals which mathematical concept was most important for each proof. This information is taken directly from the book entitled *Reciprocity Laws: From Euler to Eisenstein* by Franz Lemmermeyer.

	proof	*year*	*comments*
1.	Legendre	1788	Quadratic forms; incomplete
2.	Gauss 1	1801	Induction; April 8, 1796
3.	Gauss 2	1801	Quadratic forms; June 27,1796
4.	Gauss 3	1808	Gauss' Lemma; May 6,1807
5.	Gauss 4	1811	Cyclotomy; May 1801
6.	Gauss 5	1818	Gauss' Lemma; 1807/08
7.	Gauss 6	1818	Gauss sums; 1807/08
8.	Cauchy	1829	Gauss 6
9.	Jacobi	1830	Gauss 6
10.	Dirichlet	1835	Gauss 4
11.	Lebesgue 1	1838	$N(x_1^2 + ...x_q^2 \equiv 1 \mod p)$
12.	Schonemann	1839	Quadratic period equation
13.	Eisenstein 1	1844	Generalized Jacobi sums
14.	Eisenstein 2	1844	Gauss 6
15.	Eisenstein 3	1844	Gauss' Lemma
16.	Eisenstein 4	1845	Sine
17.	Eisenstein 5	1845	Infinite products
18.	Liouville	1847	Cyclotomy
19.	Lebesgue 2	1847	Lebesgue 1
20.	Schaar	1847	Gauss' Lemma
21.	Genocchi	1852	Gauss' Lemma
22.	Dirichlet	1854	Gauss 1
23.	Lebesgue 3	1860	Gauss 7,8
24.	Kummer 1	1862	Quadratic forms
25.	Kummer 2	1862	Quadratic forms
26.	Kedekind 1	1862	Quadratic forms
27.	Gauss 7	1862	Quadratic periods; Sept. 1796
28.	Gauss 8	1863	Quadratic periods; Sept. 1796
29.	Mathieu	1867	Cyclotomy
30.	von Staudt	1867	Cyclotomy
31.	Bouniakowski	1869	Gauss' Lemma
32.	Stern	1870	Gauss' Lemma
33.	Zeller	1872	Gauss' Lemma
34.	Zolotarev	1872	Permutations
35.	Kronecker 1	1872	Zeller
36.	Schering	1875	Gauss 3
37.	Kronecker 2	1876	Induction
38.	Mansion	1876	Gauss' Lemma

	proof	*year*	*comments*
39.	Dedekind 3	1877	Gauss 6
40.	Dedekind 3	1877	Dedekind Sums
41.	Pellet 1	1878	Stickelberger-Voronoi
42.	Pépin 1	1878	Cyclotomy
43.	Schering	1879	Gauss' Lemma
44.	Petersen	1879	Gauss' Lemma
45.	Genocchi	1880	Gauss' Lemma
46.	Kronecker 3	1880	Gauss 4
47.	Kronecker 4	1880	Quadratic period
48.	Voigt	1881	Gauss' Lemma
49.	Pellet 2	1882	Mathieu 1867
50.	Busche 1	1883	Gauss' Lemma
51.	Gegenbauer 1	1884	Gauss' Lemma
52.	Kronecker 5	1884	Gauss' Lemma
53.	Kronecker 6	1885	Gauss 3
54.	Kronecker 7	1885	Gauss' Lemma
55.	Bock	1886	Gauss' Lemma
56.	Lerch	1887	Gauss 3
57.	Busche 2	1888	Gauss' Lemma
58.	Hacks	1889	Schering
59.	Hermes	1889	Induction
60.	Kronecker 8	1889	Gauss' Lemma
61.	Tafelmacher 1	1889	Stern
62.	Tafelmacher 2	1889	Stern/Schering
63.	Tafelmacher 3	1889	Schering
64.	Busche 3	1890	Gauss' Lemma
65.	Franklin	1890	Gauss' Lemma
66.	Lucas	1890	Gauss' Lemma
67.	Pépin 2	1890	Gauss 2
68.	Pields	1891	Gauss' Lemma
69.	Gegenbauer 2	1891	Gauss' Lemma
70.	Gegenbauer 3	1893	Gauss' Lemma
71.	Schmidt 1	1893	Gauss' Lemma
72.	Schmidt 2	1893	Gauss' Lemma
73.	Schmidt 3	1893	Induction
74.	Gegenbauer 4	1894	Gauss' Lemma
75.	Bang	1894	Induction
76.	Mertens 1	1894	Gauss' Lemma
77.	Mertens 2	1894	Gauss sums
78.	Busche 4	1896	Gauss' Lemma
79.	Lange 1	1896	Gauss' Lemma
80.	de la Vallée Poussin	1896	Gauss 2
81.	Lange 2	1897	Gauss' Lemma
82.	Hilbert	1897	Cyclotomy
83.	Alexejewsky	1898	Schering
84.	Pépin 3	1898	Legendre
85.	Pépin 4	1898	Gauss 5
86.	Konig	1899	Induction
87.	Fischer	1990	Resultants
88.	Takagi	1903	Zeller
89.	Lerch	1903	Gauss 5

	proof	*year*	*comments*
90.	Mertens 3	1904	Eisenstein 4
91.	Mirimanoff and Hensel	1905	Stickelberger-Voronoi
92.	Busche 5	1909	Zeller
93.	Busche 6	1909	Eisenstein
94.	Aubry	1910	= Eisenstein 3
95.	Aubry	1910	= Voigt
96.	Aubry	1910	= Kronecker
97.	Pépin	1911	Gauss 2
98.	Petr 1	1911	Mertens 3
99.	Pocklington	1911	Gauss 3
100.	Dedekind 4	1912	Zeller
101.	Heawood	1913	= Eisensterin 3
102.	Frobenius 1	1914	Zeller
103.	Frobenius 2	1914	Eisenstein 3
104.	Lasker	1916	Stickelberger-Voronoi
105.	Cerone	1917	Eisenstein 4
106.	Bartelds and Schuh	1918	Gauss' Lemma
107.	Stieltjes	1918	Lattice points
108.	Teege 1	1920	Legendre
109.	Teege 2	1921	Cyclotomy
110.	Arwin	1924	Quadratic forms
111.	Rédei 1	1925	Gauss' Lemma
112.	rédei 2	1926	Gauss' Lemma
113.	Whitehead	1927	Genus theory (Kummer)
114.	Petr 2	1927	Theta functions
115.	Skolem 1	1928	Genus theory
116.	Petr 3	1934	Kronecker (signs)
117.	van Veen	1934	Eisenstein 3
118.	Fueter	1935	Quaternion algebras
119.	Whiteman	1935	Gauss' Lemma
120.	Dockeray	1938	Eisenstein 3
121.	Dorge	1942	Gauss' Lemma
122.	Rédei 3	1944	Gauss 5
123.	Lewy	1946	Cyclotomy
124.	Petr4	1946	Ciclotomy
125.	Skolem 2	1948	Gauss 2
126.	Barbilian	1950	Eisenstein 1
127.	Rédei 4	1951	Gauss 3
128.	Brandt 1	1951	Gauss 2
129.	Brandt 2	1951	Gauss sums
130.	Brewer	1951	Mathieu, Pellet
131.	Furquim de Almeida	1951	Finite fields
132.	Zassenhaus	1952	Finite fields
133.	Riesz	1953	Permutations
134.	Frohlich	1954	Class Field Theory
135.	Ankeny	1955	Cyclotomy
136.	D. H. Lehmer	1957	Gauss' Lemma
137.	C. Meyer	1957	Dedekind sums
138.	Holzer	1958	Gauss sums
139.	Rédei 5	1958	Cyclotomic polynomial
140.	Reichardt	1958	Gauss 3

	proof	*year*	*comments*
141.	Carlitz	1960	Gauss 1
142.	Kubota 1	1961	Cyclotomy
143.	Kubota 2	1961	Gauss sums (sign)
144.	Skolem 3	1961	Cyclotomy
145.	Skolem 4	1961	Finite fields
146.	Hausner	1961	Gauss sums
147.	Swan 1	1962	Stickelberger-Voronoi
148.	Koschmieder	1963	Eisenstein, sine
149.	Gerstenhaber	1963	Eisenstein, sine
150.	Rademacher	1964	Finite Fourier analysis
151.	Weil	1964	Theta functions
152.	Kloosterman	1965	Holzer
153.	Chowla	1966	Finite fields
154.	Burde	1967	Gauss' Lemma
155.	Kaplan 1	1969	Eisenstein
156.	Kaplan 2	1969	Quadratic congruences
157.	Birch	1971	K-theory (Tate)
158.	Reshetukha	1971	Gauss sums
159.	Agou	1972	Finite fields
160.	Brenner	1973	Zolotarev
161.	Honda	1973	Gauss sums
162.	Milnor and Husemoller	1973	Weil 1964
163.	Allander	1974	Gauss' Lemma
164.	Berndt and Evans	1974	Gauss' Lemma
165.	Hirzebruch and Zagier	1974	Dedekind Sums
166.	Rogers	1974	Legendre
167.	Castaldo	1976	Gauss' Lemma
168.	Frame	1978	Kronecker (signs)
169.	Hurrelbrink	1978	K-theory
170.	Auslander and Tolimieri	1979	Fourier transform
171.	Brown	1981	Gauss 1
172.	Goldschmidt	1981	Cyclotomy
173.	Kac	1981	Eisenstein, Sine
174.	Barcanescu	1983	Zolotarev
175.	Zantema	1983	Brauer groups
176.	Ely	1984	Lebesgue 1
177.	Eichler	1985	Theta function
178.	Barrucand and Laubie	1987	Stickelberger-Voronoi
179.	Peklar	1989	Gauss' Lemma
180.	Barnes	1990	Zolotarev
181.	Swan 2	1990	Cyclotomy
182.	Rousseau 1	1990	Exterior algebras
183.	Rousseau 2	1991	Permutations
184.	Keune	1991	Finite fields
185.	Kubota 3	1992	Geometry
186.	Russinoff	1992	Gauss' Lemma
187.	Garrett	1992	Weil 1964
188.	Motose	1993	Group algebras
189.	Rousseau	1994	Zolotarev
190.	Young	1995	Gauss sums

	proof	*year*	*comments*
191.	Brylinski	1997	Group actions
192.	Merindol	1997	Eisenstein, sine
193.	Watanabe	1997	Zolotarev
194.	Ishii	1998	Gauss 4
195.	Motose	1999	Group algebras
196.	Lemmermeyer	2000	Lebesgue 1, Ely

References

[Andrews] George E. Andrews. *Number Theory*. New York, Dover, 1994. pp.115-127 Chapter 9: Quadratic Residues

[Beiler] Albert H. Beiler. *Recreations in the Theory of Numbers: The Queen of Mathematics Entertains* (second edition). New York, Dover, 1966. pp.200-210 Chapter 19: Theorema Aureum

[Cox] David A Cox. "Quadratic Reciprocity: Its Conjecture and Application," *The American Mathematical Monthly*. May 1988. Volume 95 no.5 pp.442-448

[Komatsu] Hikosaburo Komatsu and the Mathematical Society of Japan. *Encyclopedic Dictionary of Mathematics*. London, England, The Mit Press, 2000. Volume II: 297I (Reciprocity Law)

[Lemmermeyer] Franz Lemmermeyer. *Reciprocity Laws: From Euler to Eisenstein.*Germany, Springer, 2000. Chapter 1: The Genesis of Quadratic Reciprocity

[O'Connor] J.J. O'Connor and E.F. Robertson. *Adrien-Marie Legendre http://www-groups.dcs.st-and.ac.uk/ history/Mathematicians/Legendre.html*. (March 1 2005)

[Pong] Wai Yan Pong. California State University - Dominguez Hills, Department of Mathematics *Applications of Law of Quadratic Reciprocity http://www.csudh.edu/math/wpong/m447/lqr.pdf* (Feb 26 2005)

[Roberts] Joe Roberts. *Elementary Number Theory: A Problem Oriented Approach*. London, The Mit Press, 1977. pp.192-210 Chapter 17.

[Smith] David Eugene Smith. *A Source Book in Mathematics*. New York, Dover, 1959. pp 112-119: Gauss on the Third Proof of the Law of Quadratic Reciprocity

[Stillwell] John Stillwell. *Elements of Number Theory.*New York, Springer-Verlag, 2003. Chapter 9: Quadratic reciprocity

[Weisstein] Eric W. Weisstein. *MathWorld http://mathworld.wolfram.com/*. (March 1 2005)